COOLEY LLP
MICHAEL A. ATTANASIO (151529)
(mattanasio@cooley.com)
BENEDICT Y. HUR (224018)
(bhur@cooley.com)
SIMONA AGNOLUCCI (246943)
(sagnolucci@cooley.com)
EDUARDO E. SANTACANA (281668)
(esantacana@cooley.com)
JONATHAN PATCHEN (237346)
(jpatchen@cooley.com)
ARGEMIRA FLOREZ (331153)
(aflorez@cooley.com)
NAIARA TOKER (346145)
(ntoker@cooley.com)
HARRIS MATEEN (335593)
(hmateen@cooley.com)
THILINI CHANDRASEKERA (333672)
(tchandrasekera@cooley.com)
ISABELLA MCKINLEY CORBO (346226)
(icorbo@cooley.com)
CHELSEA HU (357212)
(chu@cooley.com)
MICHAEL B. MORIZONO (359395)
(mmorizono@cooley.com)
3 Embarcadero Center, 20th Floor
San Francisco, CA 94111-4004
Telephone: (415) 693-2000
Facsimile: (415) 693-2222

Attorneys for Defendant
GOOGLE LLC

UNITED STATES DISTRICT COURT

NORTHERN DISTRICT OF CALIFORNIA

SAN FRANCISCO DIVISION

ANIBAL RODRIGUEZ, et al. individually and on behalf of all others similarly situated,

Plaintiff,

v.

GOOGLE LLC,

Defendant.

Case No. 3:20-CV-04688-RS

GOOGLE LLC'S MOTION TO DECERTIFY THE CLASS

Dept: 3, 17th Fl.
Judge: Hon. Richard Seeborg

Date Action Filed: July 14, 2020
Trial Date: August 18, 2025

TABLE OF CONTENTS

TABLE OF AUTHORITIES

Page(s)

Cases

TABLE OF AUTHORITIES
(continued)

Page(s)

TABLE OF AUTHORITIES
(continued)

Page(s)

Statutes

Other Authorities

TABLE OF AUTHORITIES
(continued)

Page(s)

TO ALL PARTIES AND THEIR ATTORNEYS OF RECORD:

Please take notice that on October 16, 2025 at 1:30 p.m. or as soon thereafter as the matter may be heard by before the Honorable Richard Seeborg of the United States District Court for the Northern District of California at the San Francisco Courthouse, Courtroom 3, 17th Floor, 450 Golden Gate Avenue, San Francisco, CA 94102, Defendant Google LLC will, and hereby does, move this this Court, pursuant to Federal Rule of Civil Procedure 23(c)(1)(C), for an order decertifying the Classes in this action.

The Motion is based on this Notice of Motion and Motion, the attached Memorandum of Points and Authorities, the pleadings and other papers filed, any oral argument, the evidence and testimony presented at trial, and any other such matters that the Court may consider. Google requests that the Court decertify both classes that were provisionally certified in this matter.

STATEMENT OF ISSUES TO BE DECIDED

1. Do individualized issues predominate, such that the Classes should be decertified for failing to satisfy Federal Rule of Procedure 23(b)(3)?
2. Are the Named Plaintiffs typical of absent class members, such that they satisfy Federal Rule of Civil Procedure 23(a)(3)?
3. Can Plaintiffs satisfy the adequacy of representation requirement of Federal Rule of Civil Procedure 23(a)(4)?

MEMORANDUM OF POINTS AND AUTHORITIES

I. INTRODUCTION

"Rule 23(c)(1)(C) requires courts to reassess class rulings as the case develops and to ensure continued compliance with Rule 23's requirements." *Amara v. Cigna Corp.*, 775 F.3d 510, 520 (2d Cir. 2014) (cleaned up). This includes during and even after trial. That the Court certified this action nearly two years ago does not insulate it from decertification when Rule 23 is no longer satisfied.

That is the case here. Trial has confirmed that the classes should be decertified. Rule 23(b)(3)'s predominance and superiority requirements are not met. Indeed, it is unclear whether Rule 23(a)(2)'s commonality requirement is even established. First, class members' individualized understandings of (s)WAA disclosures permeate several elements of Plaintiffs' claims, including whether they held an expectation of privacy over their data, whether they consented to Google's (s)WAA disclosures, and whether Google's conduct could be considered highly offensive. Second, details concerning the third-party applications (*e.g.*, the apps' terms of service, Google's agreements with the apps, the types of data that the apps collect) create endless permutations that implicate ownership under CDAFA, users' reasonable expectations of privacy, and offensiveness of the conduct. And finally, Plaintiffs' damages argument implicates highly user-dependent damages calculations.

In addition, Plaintiffs' testimony destroys typicality. Mr. Rodriguez based much of his testimony on the fact that some apps had violated Google's terms and included collection of personally-identifiable information. But the only statistical evidence showed that this occurs in 0.34% of cases, making Mr. Rodriguez atypical. And with only half as many class representatives as they had a month ago, Rule 23(a)(4) is not met.

For these reasons, class treatment is improper.[1]

II. LEGAL STANDARD

Federal Rule of Civil Procedure 23(c)(1)(C) provides that "[a]n order that grants or denies class certification may be altered or amended before final judgment." "[A] district court's order

[1] Filed concurrently with this Motion is Google's Motion for Judgment as a Matter of Law, which Google incorporates into its Motion to Decertify the Class.

denying or granting class status is inherently tentative." *Coopers & Lybrand v. Livesay*, 437 U.S. 463, 469 n.11 (1978). As such, "[d]istrict courts have a responsibility to review continually 'the appropriateness of a certified class in light of developments subsequent to class certification.'" *Abante Rooter & Plumbing, Inc. v. Alarm.com, Inc.*, 15-cv-06314-YGR, 2018 WL 558844, at *2 (N.D. Cal. Jan. 25, 2018) (quoting *Schilling v. TransCor Am., LLC*, No. 08-cv-941-SI, 2012 WL 4859020, at *1 (N.D. Cal. Oct. 11, 2012)); *Amara*, 775 F.3d at 520 ("Rule 23(c)(1)(C) requires courts to reassess class rulings as the case develops and to ensure continued compliance with Rule 23's requirements" (cleaned up)); *see also Kuehner v. Heckler*, 778 F.2d 152, 163 (3d Cir. 1985); *Richardson v. Byrd*, 709 F.2d 1016, 1019 (5th Cir. 1983). The party seeking to maintain class certification bears the burden of demonstrating that the Rule 23 requirements are satisfied, even on a motion to decertify. *See Marlo v. United Parcel Serv., Inc.*, 639 F.3d 942, 947 (9th Cir. 2011).

III. ARGUMENT

A. The Evidence Presented At Trial Reveals That Class Treatment Is Not Appropriate As Individual Issues Predominate

Federal Rule of Civil Procedure 23(b)(3) requires that, for a class seeking damages, "questions of law or fact common to class members predominate over any questions affecting only individual members, and that a class action is superior to other available methods" of adjudication. Rule 23(b)(3)'s predominance requirement "imposes stringent requirements for certification that in practice exclude most claims." *Am. Express Co. v. Italian Colors Rest.*, 570 U.S. 228, 234 (2013). To satisfy it, "plaintiffs must establish that essential elements of the cause of action . . . are capable of being established through a common body of evidence, applicable to the whole class." *Olean Wholesale Grocery Coop., Inc. v. Bumble Bee Foods LLC*, 31 F.4th 651, 666 (9th Cir. 2022) (cleaned up).

At class certification, the Court was provisionally satisfied that individual issues would not predominate over issues common to the class. Dkt. 352 at 18. Now, after Plaintiffs have fully presented their case and disclosed all the evidence behind their claims, it is clear that common evidence to establish several of the elements of Plaintiffs' class-wide claims is lacking. Individualized issues predominate.

1. Individualized Issue #1: Class Members' Particular (s)WAA-off & Third-Party App Usage

The number and variety of third-party apps and class members present a huge hurdle for Plaintiffs. Indeed, there are over 98 million class members, nearly 175 million devices, and at least 1,500 third-party apps that use Google Analytics for Firebase ("GA4F"), and scores of analytics providers. This creates endless individualized permutations with respect to numerous elements of Plaintiffs' claims, which again precludes class certification.

a) Class Members' Ownership Under CDAFA

As Google argued more fully in its Motion for Judgment as a Matter of Law, whether class members are "owners" of the at-issue data depends on specific details regarding each third-party app that uses GA4F, including the terms of service of each app and how each app operates. Plaintiffs have offered no evidence of this, neither on their own behalf, let alone for the entirety of the class.

A CDAFA claim requires that each class member be the "owner or lessee" of the (s)WAA-off data. Cal. Penal Code § 502(e). The statute does not define "owner," but it is sufficiently defined in the recent case law. The court in *Garrabrants v. Erhart* interpreted the "ownership" element of a CDAFA claim, defining it as "the right of one or more persons to possess and use a thing to the exclusion of others;" an owner is "someone who has the right to possess, use and convey something[.]" 98 Cal. App. 5th 486, 508 (2023) (cleaned up).[2] Ownership cannot be established merely by showing that data was "concerning" the plaintiff, or because the plaintiff "had some form of interest–for example, a privacy interest," in the data. *Id.* at 509; *see also Stuart v. Cnty. of Riverside*, No. 5:22-cv-00701-SPG (MARx), 2024 WL 3455263, at *19 (C.D. Cal. Apr. 22, 2024) (holding that the plaintiffs failed to establish an ownership interest in data about them stored in a government database). Rather, a plaintiff must show something concrete that gives them an ownership interest, such as "customer terms of service." *See Garrabrants*, 98 Cal. App. 5th at 510.

While Plaintiffs may assert that they, along with class members, have some form of "privacy

[2] Google acknowledges that there was a dearth of case law interpreting ownership at the time of class certification briefing. *Garrabrants* was issued in December 2023, two months after the class certification motion was argued and submitted.

interest" in the (s)WAA-off data given that it "concerns" them, this is not enough to show ownership under CDAFA, both for the Named Plaintiffs and class members. Plaintiffs are obligated to present concrete evidence, for example, that the app's terms of service and the operation of each app, that establish that *each* class member still had the "right to possess, use and convey" the (s)WAA-off data, data that is collected by the app by way of the app's incorporation of the GA4F SDK. *See* Trial Tr. Aug. 20 (Santiago) at 519:5-8 (acknowledging that each of the 42 apps Plaintiff Santiago downloaded had their own terms of service and privacy policies); Trial Tr. Aug. 25 (Rodriguez) at 842:15-21 (admitting he had a "deal with Target."); Trial Tr. Aug. 27 (Ganem) at 1260:4-14 (explaining Facebook ownership of certain app data and that the app owns the Google Analytics data). Plaintiffs have not even attempted to do so. There is no conceivable way to prove ownership via common proof. And it is obvious that this would be an administrative nightmare to collect and interpret each of the at-least 1,500 third-party apps' individual terms of service (or similar agreement) reached between every third-party app and every class member. *See Mazzei v. Money Store*, 829 F.3d 260, 272 (2d Cir. 2016) (affirming denial of class certification where "the fact-finder would have to look at every class member's loan documents to determine" which "class members *were* in fact in privity" with the defendant). The need for class-wide proof of ownership precludes class certification.

b) Reasonable Expectation Of Privacy

Plaintiffs assert that class members had a reasonable expectation of privacy. Yet the volume and variety of third-party apps, class members and analytics platforms implicated by Plaintiffs' claims destroy the propriety of class-wide treatment with respect to this element. While an expectation must be objectively reasonable, the objective test does not mean individual circumstances and behavior are irrelevant. "The extent of a privacy interest is not independent of the circumstances." *Hill v. Nat'l Collegiate Athletic Ass'n*, 7 Cal. 4th 1, 36 (1994) (cleaned up). *Hill* makes this clear: while a person in general may have a reasonable expectation of privacy as to observed urination, NCAA student-athletes have a sharply reduced expectation of privacy. *Id*. at 42-43. Class members' individual circumstances matter. And trial testimony confirms it predominates.

First, the terms of service of each individual app impact whether the apps' users had a reasonable expectation of privacy. *Garrabrants*, 98 Cal. App. 5th at 500 (explaining it is a context-specific inquiry); *Hill*, 7 Cal. 4th at 42 ("advance notice and the opportunity to consent" relevant to reasonableness of expectation of privacy). It is undisputed that Google required third-party apps that used GA4F to obtain consent from its users. Users sign up or download the apps directly from third parties, without any contact from Google. Thus, the determination as to whether there was any expectation of privacy (either an actual, subjective one or an objective, reasonable one) in the collection and transmission of (s)WAA-off data is impacted by the representations that third-party apps made to their users. Of course, if third-party apps made this clear and users consented, that would reduce—if not outright preclude—class members from having an objectively reasonable or subjective expectation of privacy. And the number of apps a user downloaded is equally relevant to the issue. One can easily imagine Google cross-examining a class member to explore the reasonableness of his or her expectation when a user had downloaded scores of apps, each of which disclosed Google's collection, after turning off (s)WAA (or having it off without even knowing it). This inquiry requires individualized proof from each third-party app that used GA4F during the class period to identify what their disclosures represented to users.

Second, the volume of third-party apps and the type of data they collect significantly impacts the reasonable expectation of privacy analysis, creating a highly-individualized inquiry. "What a user would reasonably expect in light of [the defendant's] disclosures is a relevant question, but so is the amount of data allegedly collected . . . [a]nd, the nature of the allegedly collected data[.]" *Heeger v. Facebook, Inc.*, 509 F. Supp. 3d 1182, 1193 (N.D. Cal. 2020) (cleaned up). Of course, not all apps collect the same data, have the same types of users, or deal with the same subject matter. Thus, each class member's behavior with respect to the suite of apps that the class member installed is highly relevant.

Plaintiff Rodriguez's testimony bears this out.

Q: Did you ever use the **NightOwl Companion** app while you had sWAA off?

A: Yes.

Q: Do you consider your sleep apnea a private and personal matter?

> **A**: Definitely it is.
>
> **Q**: Did you ever use the **MIPC camera** app while sWAA was off?
>
> **A**: Yes. . . . It connects to my cameras in my home.
>
> **Q**: Do you consider what you do for home security a private and personal matter?
>
> **A**: Oh, yeah, definitely.
>
> **Q**: Did you ever use the **Career Karma** app while sWAA was off?
>
> **A**: Yes.
>
> …
>
> **Q**: Do you consider whether you're looking for a new job something that's private and personal to you?
>
> **A**: Yes.
>
> …
>
> **Q**: You had no problem with the **Target** app sharing your data with Google Analytics, Adobe Analytics, or Crazy Egg; right?
>
> **A**: If -- if -- understanding how -- how I see things and what I learned, I don't think it was a big deal.
>
> **Q**: Not a big deal?
>
> **A**: Not with -- not sharing my Target information, my Target activity, with the analytics company. I don't think that's an issue.
>
> …
>
> **Q**: But you allowed **your son** to use his Android phone after you filed this complaint the same way he had used it before; right?
>
> . . .
>
> **A**: Right. He's very young. They're not using any apps like I am. They really just used it for playing games and watching videos and stuff like that. . . . . I mean, right now I would say at that time if there's any data being collected, it's a five-year-old and a ten-year-old at the time. And, again, they're not using the phone the same way as I would where you can kind of put the pieces of the puzzle together and know who I am. I think you would say it's a five-year-old and a ten-year-old, and I don't think there's much information that you can actually gather from that. It's just kids playing on a phone. It's not using apps like an adult uses an app.

Trial Tr. Aug. 25 (Rodriguez) at 812:23-813:21, 843:12-19, 856:3-5, 856:9-858:4 (emphasis added). Plaintiffs' own testimony confirms that the ***nature*** of the app, and the ***nature*** of the data collected, bear on the reasonableness of any expectation of privacy. Certain apps may create reasonable privacy expectations, others do not. Certain types of data may justify privacy

expectations, others do not. And the ***nature*** of certain users may implicate privacy issues, others not so much.

Because of the volume of different third-party apps, the varying types of data they collect, and the varied types of users of each app, individualized issues predominate in analyzing whether the class as a whole had any reasonable expectation of privacy.

Third, the role of each user with respect to their app-usage, the device and the data similarly impacts the analysis, creating even further individualized issues. In *Garrabrants*, the CEO plaintiff sued the whistleblower defendant for invasion of privacy based on the latter's alleged "accessing, taking, and subsequently retaining" the plaintiff's personal bank and tax documents. 98 Cal. App. 5th at 491. In analyzing whether an erroneous jury instruction regarding the expectation of privacy was prejudicial to the defendant, the Court of Appeal analyzed whether the jury could have found that the plaintiff had an expectation of privacy, both based on his role as a bank customer and as the bank's CEO. *Id*. at 501. As a customer, he likely had an expectation of privacy over the documents. *Id*. But since bank employees' accounts were subject to audit by the bank, as the CEO, the plaintiff may not have had an expectation of privacy. *Id*.

Here, to determine whether a user had an expectation of privacy over (s)WAA-off data, individualized information is necessary about the role each class member had with respect to each app. For instance, is a class member an employee of the third-party app's company? Does the class member use their personal device with employer device monitoring or is the class member's device subject to a "BYOD" policy? *See H.J. Heinz Co. v. Starr Surplus Lines Ins. Co.*, No. 2:15-cv-00631-AJS, 2015 WL 12791338, at *4 (W.D. Pa. July 28, 2015), *report and recommendation adopted,* 2015 WL 12792025 (W.D. Pa. July 31, 2015). Do the company's policies reduce any expectation of privacy, as in *Garrabrants*? Is the user a minor? If so, do any parental permissions over the account reduce the expectation of privacy? Moreover, each class member is a Google Account user *and* a user of at least one third-party app. Does their use of one reduce their expectation of privacy for the other? These issues further complicate the analysis and create even more individualized issues.

Fourth, the evidence showed each app uses—on average—four analytics SDKs. Trial Tr. Aug. 26 (Ganem) at 1145:18-24. Which suite of SDKs each app employs will similarly impact the

reasonableness of each class member's expectation of privacy. What data is collected by those other SDKs? Do those other SDKs "put the puzzle pieces together" as Plaintiff Rodriguez falsely claimed Google does? Trial Tr. Aug. 26 (Ganem) at 1130:16-1132:9, 1134:5-1135:15, 1136:25-1137:15; Trial Tr. Aug. 29 (Black) at 1722:1-24. Facebook does, and Adobe has no similar (s)WAA-off button. Trial Tr. Aug. 27 (Ganem) at 1260:23-1261:18, 1262:23-1263:17, 1267:9-15, 1268:9-22. Both Plaintiff Santiago and Rodriguez had the Facebook app and Mr. Rodriguez consented to Target providing his Target-app data with Adobe and an analytics provider so small that Mr. Ganem hadn't heard of it: CrazyEgg. Plaintiffs' Demonstratives at 1, 3; Trial Tr. Aug. 25 (Rodriguez) at 841:11-842:2l; Trial Tr. Aug. 27 (Ganem) at 1267:16-18. The fact that the same or similar data is captured by multiple SDKs per app makes clear that Plaintiffs have no "reasonable" expectation of privacy as to GA4F alone, or at least that it varies by individual. *Cf. McMorris v. Alioto*, 567 F.2d 897, 901 (9th Cir. 1978) (upholding courthouse magnetometer screening against privacy challenge in part because similar screening was done with respect to air travel). These individual issues predominate.

c) Offensiveness

Plaintiffs' privacy tort claims also require that they prove that Google's conduct was "highly offensive." Dkt. 445 at 9. Conduct is "highly offensive" if it is an "egregious breach of social norms" or an "intrusion [] in a manner highly offensive to a reasonable person." *See Williams v. DDR Media, LLC*, No. 22-cv-03789-SI, 2023 WL 5352896, at *5-6 (N.D. Cal. Aug. 18, 2023) (citations omitted).

The type of data is a factor that courts consider in determining whether a defendant's collection or use of user data is "highly offensive." In *McCoy v. Alphabet, Inc.*, the court dismissed the plaintiff's privacy tort claims, holding that the defendant's collection of data from third-party apps was not "highly offensive." No. 20-cv-05427-SVK, 2021 WL 405816, at *8 (N.D. Cal. Feb. 2, 2021). According to the complaint, the defendant collected "confidential and sensitive data," including how long the plaintiffs' and class members' used and had open certain apps. *Id*. The court noted that "no other types of data" were alleged to be collected, and since the app activity data "was not tied to any personally identifiable information, was anonymized, and was

aggregated," the collection did not rise "to the requisite level of an egregious breach of social norms[.]" *Id*. "Courts in this district have held that data collection and disclosure to third parties that is 'routine commercial behavior' is not a 'highly offensive' intrusion of privacy." *Hammerling v. Google LLC*, 615 F. Supp. 3d 1069, 1090 (N.D. Cal. 2022); *In re iPhone Application Litig*., 844 F. Supp. 2d 1040, 1063 (N.D. Cal. 2012) (collection of "unique device identifier number, personal data, and geolocation information" did not rise to an egregious breach of social norms).

Because offensiveness turns on *the type* of data Google collects, this then turns on what type of data third-party apps authorized to be collected. *See id*. To establish this, Plaintiffs needed to present sufficient evidence to identify the type of data each third-party app collected. Not only did Plaintiffs fail to do so, but doing so would present highly individualized analyses for each of the at-least 1,500 apps that use GA4F.

Moreover, because each app has, on average, four analytics SDK, the offensiveness of Google's conduct must be measured versus what those other analytics providers collect and do with the data so collected. Plaintiff Rodriguez made this point. After describing how he was offended by Google's data collection, he confidently declared that he would not install an app that provided data to a third-party analytics party. Trial Tr. Aug. 25 (Rodriguez) at 838:22-25. Yet, even as to Target, he consented to data collection from the Target app by Adobe and Crazy Egg. *Id*. at 842:2-21. And unlike Google, Adobe "puts the pieces together" and Mr. Rodriguez consented. Google's conduct is far from "highly offensive" if class members—like Mr. Rodriguez—consents to similar (if not even more invasive) data collection from competitive analytics platforms.

2. Individualized Issue #2: Class Members' Individual Understandings of The (s)WAA Disclosures

Plaintiffs offered no class-wide evidence about the class members' understanding of the (s)WAA disclosures. Indeed, the only evidence that Plaintiffs provided about the 98 million class members' understandings and expectations based on Google's (s)WAA disclosures are those of the Named Plaintiffs. Yet it cannot simply be assumed that *two plaintiffs'* understandings can be imputed to the entirety of the class. What class members understood about the (s)WAA disclosures is highly individualized and directly relevant to several elements of Plaintiffs' claims.

a) Expectation Of Privacy

Plaintiffs bring two privacy torts against Google: invasion of privacy under the California Constitution and intrusion upon seclusion. While the claims are technically distinct, they consist of similar elements. "The inquiry under either is whether (1) there exists a reasonable expectation of privacy, and (2) whether the intrusion was highly offensive." Dkt. 445 at 9 (cleaned up).

To establish a "reasonable expectation of privacy," a plaintiff must show: (1) an actual, subjective expectation of privacy, and (2) that the expectation was objectively reasonable. *Med. Lab'y Mgmt. Consultants v. Am. Broad. Cos.*, 306 F.3d 806, 812–13 (9th Cir. 2002); *Hill*, 7 Cal. 4th at 35.

First, each class member must have a subjective expectation of privacy. Although this Court held otherwise in its Class Certification Order, Dkt. 352 at 8 (quoting *Opperman v. Path*, No. 13-cv-00453-JST, 2016 WL 3844326, at *11 (N.D. Cal. July 15, 2016)), Google respectfully submits that the trial evidence shows this conclusion was wrong. *Opperman* cited to *Shulman v. Group W. Prods. Inc.*, 18 Cal. 4th 200, 232 (1998), for the proposition that a subjective expectation of privacy is not required. But *Shulman* proves the opposite. In reversing the Court of Appeal, the California Supreme Court identified two triable issues of fact on the reasonable expectation prong: "Whether [plaintiff] *expected* her conversations with Nurse Carnahan or the other rescuers to remain private ***and*** whether *any such expectation* was reasonable[.]" *Shulman*, 18 Cal. 4th at 233–34 (emphasis added). Thus, both an expectation and the reasonableness of the expectation are necessary components. A plaintiff must *have* an expectation before any inquiry into its reasonableness. *See Hernandez v. Hillsides, Inc.*, 47 Cal. 4th 272, 286 (2009) (the first element must be an intrusion "as to which the plaintiff ***has*** a reasonable expectation of privacy.") (citing *Shulman*, 18 Cal. 4th at 231).

The Ninth Circuit has also held as much. California follows the Restatement (2d) of Torts § 652B. *Hernandez*, 47 Cal. 4th at 286 (describing *Shulman* as "approving and following" Restatement (2d) of Torts § 652B). Interpreting Section 652B, the Ninth Circuit has held that "[t]o prevail on the first prong, the plaintiff must show (a) an actual, subjective expectation of seclusion or solitude in the place, conversation, or matter, and (b) that the expectation was objectively

reasonable." *See Med. Lab'y Mgmt.*, 306 F.3d at 812-13; *In re Facebook Internet Tracking Litig.*, 140 F. Supp. 3d 922, 933 n.5 (N.D. Cal. 2015) (same, applying California law).

The requirement of a subjective expectation of privacy is often elided, since a plaintiff in an individual action asserting a privacy claim is by definition asserting a subjective expectation of privacy. But a class action changes the calculus. In purporting to represent a class, Named Plaintiffs must establish that each class member had an expectation of privacy. And this precludes certification.

Second, Plaintiffs have completely failed to proffer any evidence of a class-wide, subjective expectation of privacy.[3] The only basis for Named Plaintiffs to claim an expectation of privacy was based on their (mis)interpretation of the (s)WAA-off disclosure.[4] Plaintiff Santiago did not share it with his friends or coworkers. Trial Tr. Aug. 20 (Santiago) at 529:17-20. And Plaintiffs offered no evidence that Plaintiffs' claimed understanding applied class-wide. *See Tyson Foods, Inc. v. Bouaphakeo*, 577 U.S. 442, 461-62 (2016); Trial Tr. Aug. 21 (Hochman) at 730:8-15 (disclaiming any expert opinion on the topic); Trial Tr. Aug. 27 (Hoffman) at 1410:8-1411:15 (pointing out that Plaintiffs' had conducted no survey). And, as discussed in Google's Motion for Judgment as a Matter of Law, that class members all had (s)WAA toggled "off," by itself, does not establish the key issue of *what* each class member *expected* when they turned (s)WAA off.

This is an individualized inquiry. First, as a threshold matter, by arguing that Google's (s)WAA disclosures created an expectation of privacy in class members, Plaintiffs must actually prove that each individual class member: 1) read the disclosure (no expectation of privacy can be created by something a user had no awareness of) and 2) reached some understanding of it (no expectation can be created by something a user did not understand). One could easily imagine a class member who just accepted when (s)WAA-off was the default, Trial Tr. Aug. 25 (Lasinski) at

[3] As the district judge who decided *Opperman* later explained, in denying class certification in a later case, "[t]he Court agrees with [defendant] that the resolution of Plaintiffs' claim under the California Constitution turns on individualized factual questions of whether each user *actually maintained* their reasonable expectation of privacy." *Hart v. TWC Prod. & Tech. LLC*, No. 20-CV-03842-JST, 2023 WL 3568078, at *9 (N.D. Cal. Mar. 30, 2023) (emphasis added).

[4] *See, e.g.*, Trial Tr. Aug. 21 (Rodriguez) at 760:3-6 ("Q. Okay. When you turned the WAA button off, did you think that Google would continue to collect and save and use your data based on everything you were doing on these apps? A. No.").

906:25-907:12, or simply clicked "no" to WAA when opening a Google Account and forming no expectation—one way or the other—as to Google's (s)WAA-off practices. *See Bahamas Surgery Ctr., LLC v. Kimberly-Clark Corp.*, 820 F. App'x 563 (9th Cir. 2020) (reversing class certification where only a subset of the class had seen and relied on the at-issue representation).

But even if Plaintiffs had shown that each class member read the disclosures and formed some understanding as to them (which they have not), they must still establish that ***each Plaintiff understood the disclosures the same way as Plaintiffs***. This is a highly individualized inquiry, as class members may have interpreted the disclosures in several different ways. Class members likely understood the disclosures correctly (*i.e.*, that (s)WAA-off governs what is saved in the user's Google Account) and formed no subjective expectation of privacy as to de-identified Google Analytics data. *See* Trial Tr. Aug. 20 (Monsees) at 391:5-22 (explaining that PX-002 showed survey participants correctly understood WAA-off). Class members may have entirely different understandings, or had understandings that changed over time. And, possibly, a given class member *may* have misunderstood the disclosures the same way that Plaintiffs did. But even as to that subset of class members, Google could probe the truth of such an assertion, testing it against such class members' other experiences with Google, their exposure to other disclosures from third-party app developers, and their own personal experience with technology. Google is entitled, as a matter of due process, to put any and all class members to their proof of an expectation.

Plaintiffs did not even try to bridge this individual proof issue. No survey. Trial Tr. Aug. 27 (Hoffman) at 1410:8-1411:15. No expert testimony. Trial Tr. Aug. 21 (Hochman) at 730:8-15. No representative samples. There is no class-wide proof of what all 98 million class members understood the (s)WAA-off disclosures to provide. The lack of class-wide proof as to *156* class members demanded decertification in *Bowerman v. Field Asset Services, Inc.*, 60 F.4th 459, 466, 469, 471 (9th Cir. 2023); *see also Castillo v. Bank of Am., NA*, 980 F.3d 723, 730 (9th Cir. 2020) (there cannot be certification for a class with "a great number of members who for some reason could not have been harmed by the defendant's allegedly unlawful conduct") (citation omitted). Plaintiffs here lack class-wide, common proof as to how *98 million class members* actually understood Google's (s)WAA-off disclosures.

b) Objectively Reasonable Expectation of Privacy

Individualized questions of class-members' understandings are also critical to the objective reasonableness of the claimed privacy expectation. Whether an expectation of privacy class-wide is reasonable is not resolved by whether named plaintiffs' lawyers can create an ambiguity in the disclosures and find a handful of named plaintiffs to vouch for that reading. Objective reasonableness must be found in broad based community norms, not esoteric interpretations. *See Sheehan v. San Francisco 49ers, Ltd.*, 45 Cal. 4th 992, 1000 (2009) ("Customs, practices, and physical settings" inform the analysis, and an expectation of privacy must be "objectively reasonable under the circumstances, especially in light of the competing social interests involved." (cleaned up)); *Halvorson v. Auto-Owners Ins. Co.*, 718 F.3d 773, 779-80 (8th Cir. 2013) (holding that the individualized determination of what was "usual and customary" for a putative class alleging breach of contract claims defeated class certification). Thus, a critical line of inquiry is how many other class members share Named Plaintiffs' expectations. The proof at trial shows only 2 out of 98 million class members.

c) Offensiveness

As discussed, *supra* III(A)(1)(c), to prevail on their tort claims, Plaintiffs must prove that Google's conduct was highly offensive. *See Williams*, 2023 WL 5352896, at *5-6.

Here, Google's collection of analytics data is common and widespread among technology companies, arguably rendering any collection of such data "routine." *See* Trial Tr. Aug. 20 (Santiago) at 523:23-524:9 ("How do we know the other [] app[s] [don't] have a Google SDK as well? **It's everything**. **It's everywhere**.") (emphasis added). Courts have explained, though, that "more routine data collection practices may be highly offensive if a defendant disregards consumers' privacy choices while simultaneously 'h[olding] itself out as respecting' them." *See In re Vizio, Inc., Consumer Priv. Litig.*, 238 F. Supp. 3d 1204, 1233 (C.D. Cal. 2017) (quoting *In re Nickelodeon Consumer Priv. Litig.*, 827 F.3d 262, 292 (3d Cir. 2016)) (emphasis added). Thus, Plaintiffs' claim of "offensiveness" of Google's routine data collection practice largely turns on whether it simultaneously held itself out as respecting consumers' privacy choices, when in reality disregarding them. *See Vizio*, 238 F. Supp. 3d at 1233. But this assumes, of course, that users

perceived from Google's (s)WAA disclosures that (s)WAA-off actually applied to GA4F data from third-party apps. *See id*. Equally relevant to disproving offensiveness would be if many class members correctly understood what (s)WAA-off applied to and that Google honored the promise it made.

Because offensiveness turns on specific facts about class members' beliefs and understandings, it is again a highly individualized inquiry inappropriate for class treatment.

d) Loss Or Damage Under CDAFA

Plaintiffs' CDAFA claim requires proof of "loss or damage" from the allegedly unpermitted access to data. While the question of permission is viewed from Google's perspective, *see* Dkt. 661 at 5, the question of "loss or damage" is based on what class members suffered. Even if (counterfactually) Google understood that (s)WAA-off revoked permission to collect (s)WAA-off data, and (again, counterfactually) Google disregarded that revocation for a given class member, that class member still does not suffer "loss or damage" if the class member did not also expect or understand (s)WAA-off to withdraw permission. *Cf. Mirkin v. Wasserman*, 5 Cal.4th 1082, 1088-92 (1993) (explaining that a plaintiff must prove *actual reliance* on a misrepresentation in order to "establish a complete causal relationship" between the alleged misrepresentation and harm) (citation omitted).

e) Consent

Consent is an affirmative defense to Plaintiffs' privacy claims. The Ninth Circuit has held that Google's policies unambiguously disclose its user activity data in third-party apps. *See Hammerling v. Google, LLC*, No. 22-17024, 2024 WL 937247, at *2 (9th Cir. Mar. 5, 2024). Because Google's third-party app data collection is unambiguously disclosed–and thus created a baseline of consent–the only way for Plaintiffs to prove that class members did not consent to the collection of (s)WAA-off data is to show that each (mis)understood Google's disclosures in the same way Plaintiffs do.

In *Hammerling*, Google's privacy policy explained that it "collect[ed] data on 'third-party … apps that use [Google's] services.'" 2024 WL 937247, at *1. The Ninth Circuit held that, "[r]ead **in the context of the Policy as a whole**, the phrase . . . **unambiguously discloses** Google's

collection of user activity data in third-party apps." *Id*. (emphasis added).

As in *Hammerling*, Google here unambiguously disclosed that (s)WAA-off data may still be collected by third-parties and sent to Google. In the "Activity Controls" page of a user's Google Account settings (where the "Web & App Activity" setting can be toggled on or off), Google explains that the settings therein can be used to "[c]hoose which settings will save data **in your Google Account**." PX-084 at 1 (emphasis added). Google further disclosed that "[i]f Web & App Activity is turned on, your searches and activity from other Google services are saved **in your Google Account**." PX-113 at 1 (emphasis added). Finally, in Google's general Privacy Policy, it discloses to users that "a website might use our . . . analytics tools (**like Google Analytics**) . . . These services **may share information** about your activity with Google . . ." PX-062 at 22 (emphasis added). "[I]n the context of the Polic[ies] as a whole," Google's representations "unambiguously disclose[]" that the WAA/(s)WAA settings *only* pertain to data saved to a user's Google Account, and that third-party apps may collect and transmit data to Google. *See Hammerling*, 2024 WL 937247, at *2.

Since Google unambiguously disclosed its third-party app data policies as a matter of law,[5] the only way for class members to defeat consent is if a class member read and understood the (s)WAA disclosures in the same way as Plaintiffs. Again, this requires establishing the subjective understanding of each class member, rendering class treatment improper.

3. Individualized Issue #3: There Are Individualized Issues Within The iOS Class

Even within the iOS Class (Class 2), there are significant permutations based on differing features of the iOS system over time.

The iOS Class ran from July 1, 2016 to September 23, 2024. Yet, starting in 2021 upon the rollout of iOS 14.5, Apple implemented a feature preventing Google from knowing whether iOS users were Google users. Professor John Black explained, in iOS 14.5, Apple implemented a new

[5] Upon turning (s)WAA off, Google explained to users that "Pausing additional Web & App Activity may limit or disable more personalized experiences across Google services. For example, you may stop seeing helpful recommendations based on the apps and sites you use. . . . Visit [link] to change this and your other Google Account settings and **learn about the data Google continues to collect and why** at [link]." G0607 at 6-7 (emphasis added).

policy where iOS users would receive a notification upon using an app. Trial Tr. Aug. 29 (Black) at 1706:17-23. The pop-up would ask the user: "Ask app not to track." *Id*. at 1706:18-23. If a user enabled this feature, then Google would not be sent a user's device ID (specifically, "IDFA"). *Id*. Without the IDFA, Google would not be able to perform a consent check, and thus could not determine whether an iOS user was a Google user. *Id*. at 1707:4-10.[6] Professor Knittel testified similarly, and added that without a user's IDFA, Google treats the user's data as if the user is "signed out," meaning it is de-identified. Trial Tr. Aug. 28 (Knittel) at 1563:23-1564:8, 1579:21–23. This creates further individualized issues, even within just the iOS Class. For example, for every user within the iOS Class, did they start using third-party apps with (s)WAA off before or after 2021? If after 2021, did they install iOS 14.5? If so, for which apps did they enable the "ask app not to track" feature?

First, these issues impact the analysis of whether Google acted "without permission" with respect to Plaintiffs' CDAFA claim. To prevail on their CDAFA claim, Plaintiffs must show that Google's collection of (s)WAA-off data was "without permission." Cal. Penal Code § 502(c)(2). Further, Google must have "knowingly" acted without permission. *See id*.; *Facebook, Inc. v. Power Ventures, Inc.*, 844 F.3d 1058, 1069 (9th Cir. 2016); *People v. Hawkins*, 98 Cal. App. 4th 1428, 1438-39 (2002) ("Knowingly" applies to all elements of Section 502(c)(2), not just access). The implementation of iOS 14.5 complicates this analysis, as Plaintiffs may need to establish whether Google was aware that users enabled the "ask app not to track" feature, for which apps, and what Google subsequently did with that information.

Second, and similarly, this impacts the analysis as to whether members of the iOS Class consented to Google's conduct. Plaintiffs may have to show whether Google was aware that users enabled the "ask app not to track" feature, for which apps, whether this constituted revocation of user consent to collect data, and whether any such consent revocation with respect to the iOS system could be imputed to Google as well.

[6] If a user allows an app to track, Google is still unable to determine whether a user is (s)WAA-on or (s)WAA-off without violating the "core principle" of not mixing pseudonymous data with an identifier. Trial Tr. Aug. 29 (Black) at 1707:11-22.

4. Individualized Issue #4: Plaintiffs' Actual Damages Calculations

Google objected to Plaintiffs' actual damages theory via both a *Daubert* motion and at class certification. This Court disagreed and certified a class based on an "actual damage" theory of a *one-time* $3 payment per device. Google does not waive those objections. But whatever other issue existed with Plaintiffs' actual damages model, it at least had the upside of avoiding questions of individual proof of how much or how often each class member used their devices. But Plaintiffs now walk from that model; they have asked for a multiple of that $3 per device figure based on some number of months. Trial Tr. Aug. 19 (Pls.' Opening) at 225:16-226:19.

But by asking for a multiplier by some number of months, Plaintiffs destroy common-proof. Why is "months" of (s)WAA-off relevant or probative of actual harm? No expert opinion as to that. Why not the amount of app usage? More fundamentally, if the number of months of (s)WAA-off is a relevant consideration in the calculation of damages, then that presents an *individual* question: how many months did each class member have (s)WAA-off? *See Lara v. First Nat'l Ins. Co. of Am.*, 25 F.4th 1134, 1139 (9th Cir. 2022) (holding that predominance was destroyed where individualized damages inquiries were required); *In re Apple iPhone Antitrust Litig.*, No. 11-cv-6714-YGR, 2022 WL 1284104, at *16 (N.D. Cal. Mar. 29, 2022) ("to survive the predominance inquiry" plaintiffs must "establish that 'there is a method, common across the class, for arriving at individual damages'" (citation omitted)). Plaintiffs have no expert testimony that a month-multiplier is an accurate way to estimate damage per class member. And certainly a given class member could not prove actual harm at trial by multiplying $3 by whatever number of months are suggested by plaintiffs' counsel at argument. *See Tyson Foods*, 577 U.S. at 460-61. Because Plaintiffs have already asked, in opening, for a month-multiplier of Mr. Lasinski's "one time" $3 payment, the Court should decertify the class.

B. The Requirements Of Rule 23(a) Are Not Satisfied

Federal Rule of Civil Procedure 23(a) requires that, for every type of class, the following requirements be met: (1) numerosity, (2) commonality, (3) typicality, and (4) adequacy of representation. The Court provisionally found that all of these requirements had been met. Dkt. 352. However, as the evidence admitted at trial has shown, there are serious questions about

whether Plaintiffs have actually satisfied these requirements.

1. Inclusion Of Users' Personally-Identifiable Information In (s)WAA-Off Data Is Not An Issue Common To The Class

Class treatment is only appropriate for "questions of law or fact common to the class." Fed. R. Civ. P. 23(a)(2). This requirement, colloquially referred to as "commonality," requires that each class member suffer the same injury. *Wal-Mart Stores, Inc. v. Dukes*, 564 U.S. 338, 349-50 (2011) (citing *Gen. Tel. Co. of Southwest v. Falcon*, 457 U.S. 147, 157 (1982)). With respect to injury based on the inadvertent inclusion of users' names, email addresses, and phone numbers in (s)WAA-off data sets, commonality is not satisfied under Rule 23(a)(2).

A central contention of Plaintiff Rodriguez's testimony was that his name, email address and phone number, considered personal information by the parties, were included in (s)WAA-off data sets provided to Plaintiffs. "My name, my email address, my phone number is all there." Trial Tr. Aug. 25 (Rodriguez) at 826:10. Yet this is not how the collection of (s)WAA-off data is designed to work. As David Monsees testified, "[W]hen you had WAA off, we would log those logs generated . . . but always to a de-identified ID that happened to be the exact same ID as when you're using Google signed out of your Google Account." Trial Tr. Aug. 20 (Monsees) at 385:4-12. Rather, the inclusion of personally-identifiable information is "extraordinarily rare." Trial Tr. Aug. 29 (Black) at 1712:3-7. Across 132,000 data sets analyzed by Professor Black, only 0.34% included the user's email, and each of these instances was Plaintiff Rodriguez's. *Id*. at 1720:12-15. Indeed, the exemplar data sets admitted as evidence include personally-identifiable information for only 4 out of the 52 individuals' data that was included. *Id*. at 1712:8-11. Even this is a proportion far higher than what actually occurs. *Id*. at 1712:8-11.

The Named Plaintiffs' testimony further establishes that this is not a class-wide issue. Plaintiff Rodriguez himself explains, "I mean, ***with me specifically***, it's pretty much you know it's me. My name's in there. . . . [H]ow is it de-identified if my name, my email, my phone number is in there?" Trial Tr. Aug. 25 (Rodriguez) at 826:1-4 (emphasis added). And Plaintiff Santiago never alleged that any of his personal, de-identified information was included in the (s)WAA-off data sets.

Commonality cannot be established for this issue. Any injury due to a class member's personally-identifiable information inadvertently included in (s)WAA-off data sets cannot be imputed across the class.

2. Plaintiff Rodriguez's Claims Are Not Typical Of The Class Because His Personally-Identifiable Information Was Inadvertently Included In (s)WAA-Off Data

To satisfy Rule 23(a), the "claims or defenses of the representative parties [must be] typical of the claims or defenses of the class." Fed. R. Civ. P. 23(a)(3). The evidence admitted at trial demonstrates that the Named Plaintiffs' claims are not typical of the class.

As discussed above, *supra* III(B)(1), Plaintiff Rodriguez's claims are based on the inclusion of his personally-identifiable information in (s)WAA-off data sets. Trial Tr. Aug. 25 at 826:10. This is "extraordinarily rare" and not how the collection of (s)WAA-off data is designed to work. Trial Tr. Aug. 29 (Black) at 1712:3-7; Trial Tr. Aug. 20 (Monsees) at 385:4-12. Even Plaintiff Rodriguez agreed that his situation was unique: "My name's in there. There -- I mean, de-identified, it's how -- how is it de-identified if my name, my email, my phone number is in there? ***So in my case***, it's -- it doesn't matter because it's all there." Trial Tr. Aug. 25 (Rodriguez) at 825:23-826:5 (emphasis added). Because this occurred with such a low percentage of the sampled data, and there is no evidence of how many class members were impacted, there is no basis to conclude that Plaintiff Rodriguez's claims are typical of the class. And because he is the sole representative of the Android class who appeared at trial, his lack of typicality requires decertification of (at the very least) the Android-class.

3. The Circumstances Just Before And During Trial Indicate That The Adequacy Of Representation Requirement Is Not Satisfied

Federal Rule of Civil Procedure 23(a)(4) requires that "the representative parties will fairly and adequately protect the interest of the class." Based on events leading up to and during trial, this latter requirement is seriously called into question.

Two months before trial, there were four named plaintiffs. Each had been deposed. Each had sworn they would be at trial. Then, just weeks before trial, Sal Cataldo sought (and was granted) leave to be relieved as class counsel. No explanation was given. The weekend before

trial, Susan Harvey was in San Francisco to prepare for and attend trial. Dkt. 611 at 1. But Ms. Harvey disappeared under ill-explained circumstances. Trial Tr. Aug. 20 at 344:13-16. Trial began with only two out of the original four Named Plaintiffs in the courtroom. The first of the remaining two, Julian Santiago, admitted on the stand that his lawyers misrepresented facts to him. Trial Tr. Aug. 20 (Santiago) at 513:1-5 (**Q**: You just said it was misrepresented three minutes ago. Who misrepresented it to you? **A**: If – my previous counsel. **Q**: Your current counsel. **A**: My – yeah. Counsel who spoke previously, yes.). The final Named Plaintiff, Anibal Rodriguez, focused his testimony on a theory of harm–the "puzzle piece" theory–that even Plaintiffs' technical expert disclaimed. Trial Tr. Aug. 21 (Hochman) at 735:21-739:20. Nor is Mr. Rodriguez's situation of his apps providing improper data to Google typical of class claim.

These events raise serious doubts about the adequacy of the remaining class representatives and class counsel under Rule 23(a)(4).

IV. CONCLUSION

For the reasons stated above, Google respectfully requests that the Court decertify both Plaintiffs' damages and injunctive classes.

Dated: September 1, 2025

Respectfully submitted,

COOLEY LLP

By: */s/ Jonathan Patchen*

Michael A. Attanasio
Benedict Y. Hur
Simona Agnolucci
Eduardo E. Santacana
Jonathan Patchen
Argemira Flórez
Naiara Toker
Harris Mateen
Thilini Chandrasekera
Isabella McKinley Corbo
Chelsea Hu
Michael B. Morizono

Attorneys for Defendant Google LLC